user-spoken transaction identifier is compared with the computer transaction identifier, and the user-spoken verification identifier is compared with a voice print of the user. An authentication message is transmitted to the computer if the user-spoken transaction identifier matches the computer-generated transaction identifier and if the user-spoken verification identifier matches the voice print.

Claim 27 is directed to a system for authenticating an electronic transaction between a first user-operated device and a computer. The computer is configured to conduct electronic transactions. The system includes a voice browser configured to receive and process user-spoken information when coupled to a second user-operated device, such as a telephone. The voice browser is programmed to compare a user-spoken transaction identifier to a computer-generated transaction identifier, and to compare a user-spoken verification identifier to a voice print of the user. A session correlator is coupled to the voice browser. The session correlator is configured to transmit an authentication message to the computer if the user-spoken transaction identifier matches the computer transaction identifier, and if the user-spoken verification identifier matches the voice print.

Claim 63 is directed to a computerized voice verification method for authenticating an electronic transaction between a user and a computer. The computer is configured to conduct electronic transactions. The method includes enrolling the user in a voice verification system whereby the user provides the system with a user voice print. The electronic transaction is performed. A transaction identifier is received from the computer via an electronic data link in response to performing the electronic transaction. A user-spoken transaction identifier is received. A user-spoken verification identifier is also transmitted by the user via a voice connection. The user-spoken transaction identifier is compared with the computer transaction identifier and the user-spoken verification identifier is compared with a voice print of the user. An authentication message is transmitted to the computer if the user-spoken transaction identifier matches the computer transaction identifier and if the user-spoken verification identifier matches the voice print.

Claim 65 is directed to a computerized method for controlling web-site navigation. The method includes providing an authentication system having a voice recognition unit and a session correlator. The voice recognition unit has access to a pre-registered voice print of the user. The authentication system is coupled to a user computer and a web-site during the computerized method. A transaction is conducted between the user computer and the web-site. The web-site transmits a transaction identifier to the user computer and the

2

authentication system in response to the transaction. A user-spoken transaction identifier and a user-spoken verification identifier is received via a telephonic connection. The authentication system is programmed to compare the user-spoken transaction identifier to the transaction identifier and the user-spoken verification identifier to the pre-registered voice print. An authentication message is transmitted to the web-site if the user-spoken transaction identifier matches the transaction identifier and if the user-spoken verification identifier matches the voice print. At least one user-spoken command is received for controlling web-site navigation. The authentication system is programmed to convert the at least one user-spoken command into at least one computer-readable command. The at least one computer readable command is transmitted to the web-site. The at least one computer readable command is executed by the web-site, such that the user controls web-site navigation of the web-site by the at least one user-spoken command.

Hoffman is directed to a tokenless biometric electronic identification system. Referring to Figure 1 and the associated text in column 5, the system includes data processing center (DPC) 8 coupled to various networks, via firewall machine 26. DPC 8 includes memory data bank 12, various biometric databases, and comparator engine 30. Each of these elements are coupled to execution module 28. Data bank 12 stores audio signatures that identify transaction processors 24 (AMEX, Master Card, VISA, etc.). See column 8, lines 21-67. The biometric databases store user biometrics, such as retinal scans, voice prints, or whatever. During registration, the biometric is linked with a transaction processor. A PIN code may be employed during registration for increased security. See column 7, line 59 – column 8, line 11. The biometric is also linked with account information. See column 8, lines 13 – 16.

In light of the Examiner's comments, perhaps it would be helpful to review the process disclosed by Hoffman. The process is shown in Figure 2 and described at col. 6, line 31 – col. 7, line 57. When the user chooses to execute an electronic transaction, the user provides DPC 8 with a biometric sample (e.g. the user's voice). The comparator engine compares the sample with the voice biometric stored during registration. If there is a match, the transaction is allowed to proceed, and the account information and the details of the transaction are forwarded to the transaction processor (e.g., a bank, AMEX, etc.). After the transaction is complete, DPC 8 transmits the audio signature code of the transaction processor back to the user terminal. The user terminal plays the audio signature of the transaction processor back to the user in response to receiving the audio signature code.

3

According to **MPEP 2131**, "to anticipate a claim, the reference must teach every element of the claim." A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Claim 1 and Claim 63:

Claim 1 is a computerized method for authenticating a transaction between a user and a computer, the computer being configured to conduct electronic transactions. Claim 63 is a computerized voice verification method for authenticating an electronic transaction between a user and a computer.

While the Examiner maintains the rejection, he has failed to point out where Hoffman discloses the step of receiving a computer generated transaction identifier from the computer via an electronic link, as recited in claim 1 and claim 63. The Examiner argues that the recited computer generated transaction identifier reads on the voice biometric disclosed by Hoffman. On its face, this argument cannot be true because a computer generated transaction identifier necessarily is typically digital computer data, whereas a voice biometric is analog sound waves.

As noted previously, the Examiner maintains that the step of receiving a user-spoken transaction identifier and a user spoken verification identifier transmitted by the user via a voice connection is anticipated by col. 2, lines 45-59. However, the cited text discloses a system that includes a biometric database and a comparator. The comparator compares a user-biometric sample with at least one registered biometric sample. An audio signature associated with the transaction processor (AMEX, VISA, etc.) is also stored in the system. The computer is configured to play back the audio signature to the user to identify the transaction processor. For example, the audio signature is played back to communicate to the user that he/she is trying to conduct a transaction with his/her VISA card. Thus, Hoffman teaches the use of only one biometric voice sample. The Examiner has failed to point out where Hoffman teaches or discloses the step of receiving a user-spoken transaction identifier and a user spoken verification identifier transmitted by the user via a voice connection, as recited in claim 1 and claim 63.

The examiner repeats his assertion that the Abstract and lines 3 – 7 anticipate a step of comparing the user spoken transaction identifier with the computer transaction identifier. However, this portion of the text only states that a comparator compares a bid biometric sample to at least one registered biometric sample. As noted above, the applicant points out

4

that the Examiner has failed to point out where Hoffman discloses the step of receiving a computer generated <u>transaction</u> identifier from the computer via an electronic link. The Examiner seems to be confusing the audio signature of the transaction processor with the computer generated transaction identifier. Clearly, the audio signature identifies the transaction processor whereas the transaction identifier is generated for each transaction. Thus, the Examiner has failed to point out where Hoffman discloses the step of comparing the user spoken transaction identifier with the computer transaction identifier, as recited in claim 1 and claim 63.

The examiner restates his assertion that the Abstract and col. 3, lines 6-23 disclose the step of transmitting an authentication message to the computer if the user spoken transaction identifier and the user spoken verification identifier matches the voice print. The Applicants noted in their last response, and re-assert here, that this verbiage is not an accurate representation of the claim language. The cited text merely teaches that a user provide a biometric bid sample which is compared to a registered biometric sample. The system also plays back the audio signature of the transaction processor. The user only provides one biometric bid sample. Thus, the Examiner has failed to point out where Hoffman discloses the step of transmitting an authentication message to the computer if the user-spoken transaction identifier matches the computer-generated transaction identifier <u>and</u> if the user-spoken verification identifier matches the voice print, as recited in claim 1 and claim 63.

The examiner also states that Hoffman discloses a matching password in column 4, lines 58-67. Referring column 5, lines 5-14, and column 7, line 60 – column 8, line 11, PINS may be employed by the user during to enhance security during the registration process. They are not used during the transaction. Referring to the second step of Figure 2, the user enters only one "Bid Biometric Sample."

For the above reasons, the applicant believes that claims 1-26 and 63-64 are patentable under 35 U.S.C. § 102(e).

Claim 27:

As noted in the Applicants' last response, the Examiner has failed to provide a *prima facie* case of anticipation with respect to claim 27 because the Examiner has failed to provide an independent examination of this claim.

Previously, the Applicants pointed out that the Examiner did not specify how Hoffman applies to claim 27. In response, the Examiner points to col. 10, lines 31 – 47 for

support for his rejection. However, the paragraph cited by the Examiner does not disclose a voice browser or a session correlator as recited in the claims.

Col. 10, lines 31 – 47 describes the term "audio signature." The cited text states that "[t]he audio signature may be in the form of an audible voice..." The only hardware discussed in the text is the transaction processor, which the bank's computing facility. The Examiner also states that Hoffman discloses a token-based biometric that may be fingerprints or voice prints. Actually, Hoffman discloses a tokenless biometric. However, the actual title of the invention is irrelevant, because the Examiner must point out where each element can be found in claim 27 and he has failed to do so. Therefore, the Examiner has not made a prima facie case of anticipation because the Examiner has failed to point out where Hoffman discloses a voice browser and a session correlator.

For the above reasons, the applicant believes that claims 27 - 62 are patentable under 35 U.S.C. § 102(e).

Claim 65:

As noted in the last response, The Examiner has failed to provide a *prima facie* case of anticipation with respect to claim 65 because the Examiner has failed to provide an independent examination of this claim. In the Examiner's response to the Applicants' arguments, the Examiner argues that claim 65 is anticipated by "firewall machine 26," as shown in Figure 1. In col. 6, lines 25 – 29, Hoffman states that firewall machine 26 "filters out all messages that are not from legitimate terminal devices." As will be seen in the discussion below, a firewall does not perform web-site navigation.

Claim 65 is a computerized method for controlling web-site navigation. The Examiner has failed to point out where or how firewall 26 performs the step of conducting a transaction between the user computer and the web-site, wherein the web-site transmits a transaction identifier to the user computer and the authentication system in response to the transaction. The Examiner has failed to point out where or how firewall 26 performs the step of receiving at least one user-spoken command to control web-site navigation, as recited in claim 65. The Examiner has failed to point out where or how firewall 26 performs the step of transmitting the at least one computer readable command to the web-site. The Examiner has failed to point out where or how firewall 26 performs the step of executing the at least one computer readable command, such that the user controls web-site navigation by the at least one user-spoken command.

Thus, the Examiner has failed to make a prima facie case of anticipation with respect to claim 65. For the above reasons, the applicant believes that claims 65-68 are patentable under 35 U.S.C. § 102(e).

2. Response to the Examiner's Arguments.

a.) In the Applicants last response, the Applicants pointed out that Hoffman does not disclose the step of receiving a computer generated transaction identifier from a computer via an electronic data link.

The Examiner responds by asserting that this step is performed by Hoffman when the user's biometric sample is obtained by the user. The Applicants have provided a detailed discussion of the process employed by Hoffman in the discussion of the Hoffman reference provided above. The Applicants urge the Examiner to directly compare the claim language to the steps performed by Hoffman. While the Examiner correctly states that Hoffman teaches the step of receiving a biometric sample from the user, this only corresponds to half of the second step recited in claim 1, i.e., "receiving ...a user-spoken verification identifier." The user-spoken verification identifier is later compared with a stored voice print. Applicants note that the step recited prior thereto is the step of "receiving a computer-generated transaction identifier." This identifier is compared with a user spoken transaction identifier. The only step that Hoffman fully discloses is the step of comparing a user-spoken verification identifier with a stored voice print. Hoffman does not disclose, teach, or suggest the other steps recited in claim 1. Thus, as Applicants have pointed out, with regard to claim 1 and claim 63, the Examiner has failed to make a prima facie case of anticipation.

b.) Applicants have previously pointed out that Hoffman does not disclose a voice browser or a session correlator, as recited in claim 27. In response, the Examiner points to col. 10, lines 31 – 47 for support for his rejection.

As pointed out above, the paragraph cited by the Examiner does not disclose a voice browser or a session correlator as recited in claim 27. In fact, col. 10, lines 31 – 47 describes the meaning of the term "audio signature." The cited text states that "[t]he audio signature may be in the form of an audible voice..." The only hardware discussed is the transaction processor, which refers to the financial entity's computer (i.e., a bank, AMEX, etc.). Also noted above, the Examiner asserts that Hoffman discloses a "token-based biometric." Again, Hoffman discloses a tokenless biometric. In any case, the Examiner must point out where

each element can be found in claim 27 and he has failed to perform this task. Therefore, has not made a prima facie case of anticipation.

c.) With respect to claim 65, Applicant has previously argued, both above and in the last response, that Hoffman does not disclose a computerized method for controlling web-site navigation. The method includes the steps of: conducting a transaction between the user computer and the web-site, wherein the web-site transmits a transaction identifier to the user computer and the authentication system in response to the transaction; receiving at least one user-spoken command to control web-site navigation; transmitting the at least one computer readable command to the web-site; and executing the at least one computer readable command, such that the user controls web-site navigation by the at least one user-spoken command.

Again, the Examiner argues that this claim is anticipated by "firewall machine 26," as shown in Figure 1. Hoffman states that firewall machine 26 "filters out all messages that are not from legitimate terminal devices." As pointed out above, the Examiner has failed to show how firewall machine 26 performs the method steps recited by claim 65. Thus, with regard to claim 65, the Examiner has failed to make a prima facie case of anticipation.

3. Conclusion

Based upon the remarks and papers of record, Applicant believes the pending claims of the above-captioned application are in allowable form and patentable over the prior art of record. Applicant respectfully requests reconsideration of the pending claims 1-68 and a prompt Notice of Allowance thereon.
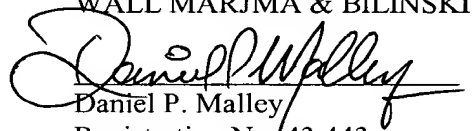
Applicant believes that no extension of time is necessary to make this Response timely. Should Applicant be in error, Applicant respectfully requests that the Office grant such time extension pursuant to 37 C.F.R. § 1.136(a) as necessary to make this Response timely, and hereby authorizes the Office to charge any necessary fee or surcharge with respect to said time extension to the deposit account of the undersigned firm of attorneys, Deposit Account 13-2491.

Please direct any questions or comments to Daniel P. Malley at (607) 256-7307.

Respectfully submitted,

WALL MARJMA & BILINSKI

Date: 6/30/03

Daniel P. Malley
Registration No. 43,443
WALL MARJMA & BILINSKI
101 S. Salina Street
Suite 400
Syracuse, NY 13202